SEALED FILED

UNITED STATES DISTRICT COURT

JAN 2 8 2020

CLERK, U.S DISTRICT COURT
EASTERN DISTRICT OF CALIFORNIA
BY _____ DEPUTY CLERK

for the

Eastern District of California

In the Matter of the Search of)
)
)
The person of WILLIAM SASSMAN)
)
)

Case No. 2:20-SW 0100 KJN

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SEE ATTACHMENT A-2, attached hereto and incorporated by reference.

located in the Eastern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B, attached hereto and incorporated by reference

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 1956 and 1957	Money Laundering and Conspiracy
18 U.S.C. § 1343	Wire Fraud
18 U.S.C. § 1344	Bank Fraud
18 U.S.C. § 1349	Conspiracy to Commit Wire and Bank Fraud
18 U.S.C. § 1030	Fraud and Related Activity in Connection with Computers

The application is based on these facts:

SEE AFFIDAVIT, attached hereto and incorporated by reference.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice _____ days (give exact ending date if more than 30 _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Allison Boos, Special Agent
Federal Bureau of Investigation
Printed name and title

Sworn to before me and signed in my presence.
Date: Jan 27, 2020

Judge's signature

City and state: Sacramento, California

Kendall J. Newman, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT

I, Allison Boos, being duly sworn, hereby depose and state as follows:

I. INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation and have been since March 2019. During the course of my employment with the FBI, I have received training in a variety of investigative and legal matters, including the topics of Fourth Amendment searches and seizures. I have a bachelor's degree in computer science and a master's degree in information security. I presently am assigned to a squad dedicated to computer intrusions. In my current position as an FBI Special Agent, I am responsible for, among other things, investigating criminal violations of federal statutes covering fraud and related activities in connection with computers. Pursuant to 18 U.S.C. $ 3052, I have statutory authority to apply for and execute search warrants.

II. PURPOSE

2. The facts in this Affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This Affidavit is intended to show that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. Rather, I make this affidavit in support of an application for a warrant to search:

(1) 1255 University Avenue, Unit 221, Sacramento, CA 95825 (hereafter referred to as the "SUBJECT RESIDENCE"), further described in Attachment A-1;

(2) The Person of William SASSMAN, further described in Attachment A-2;

(3) 5150 Fair Oaks Blvd., Suite 101-256, Carmichael, CA 95608, (hereafter referred to as the "SECONDARY SUBJECT LOCATION"), further described in Attachment A-3;

and,

the seizure of the items described in Attachment B.

III. OVERVIEW

3. During this investigation, Federal Law Enforcement Officers have determined that William SASSMAN received funds that were stolen from the Tukwila School District in the state of Washington. The funds were stolen as part of a Business E-mail Compromise ("BEC") scam, in which fraudster(s) impersonated a contractor for the school district and tricked the school district into sending approximating $6,558,955.31 to a bank account controlled by SASSMAN. Though it is unclear who was responsible for sending the fraudulent email instructions to the school district, there is probable cause that SASSMAN conspired with others to receive these stolen funds, some of which he spent on personal items, such as computers, gasoline, and credit card payments. The alleged violations are:

   a. Money Laundering and Conspiracy, in violation of Title 18, United States Code, Sections 1956 and 1957.

   b. Wire Fraud, in violation of Title 18, United States Code, Section 1343;

   c. Bank Fraud, in violation of Title 18, United States Code, Section 1344;

   d. Conspiracy to Commit Wire and Bank Fraud, in violation of Title 18, United States Code, Section 1349; and

   e. Fraud and Related Activity in Connection with Computers, in violation of Title 18, United States Code, Section 1030.

IV. TECHNICAL BACKGROUND

4. Digital currency (also known as crypto-currency) is generally defined as an electronic-sourced unit of value that can be used as a substitute for fiat currency (i.e. currency created and regulated by a government.) Digital currency exists entirely on the Internet and is not stored in any physical form. Digital currency is not issued by any government, bank, or company and is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Digital currency is not illegal in the United States and may be used for legitimate financial transactions. However, digital currency is often used for conducting illegal transactions, such as the sale of controlled substances.

5. Bitcoin[1] is a type of digital currency. Bitcoin payments are recorded in a public ledger that is maintained by peer-to-peer verification and is thus not maintained by a single administrator or entity. Individuals can acquire Bitcoin either by "mining" or by purchasing Bitcoin from other individuals. An individual can "mine" for Bitcoins by allowing his/her computing power to verify and record the Bitcoin payments into a public ledger. Individuals are rewarded for this by being given newly created Bitcoins.

6. An individual can send and receive Bitcoins through peer-to-peer digital transactions or by using a third-party broker. Such transactions can be done on any type of computer, including laptop computers and smart phones.

7. Bitcoins can be stored in digital "wallets." A digital wallet essentially stores the access code that allows an individual to conduct Bitcoin transactions on the public ledger. To access Bitcoins on the public ledger, an individual must use a public address (or "public key") and a private address (or "private key.") The public address can be analogized to an account number while the private key is like the password to access that account.

8. Even though the public addresses of those engaging in Bitcoin transactions are recorded on the public ledger, the true identities of the individuals or entities behind the public addresses are not recorded. If, however, a real individual or entity is linked to a public address, it would be possible to determine what transactions were conducted by that individual or entity. Bitcoin transactions are, therefore, described as "pseudonymous," meaning they are partially anonymous.

9. A Business E-mail Compromise ("BEC") is a sophisticated scam using e-mail and/or other electronic communication which impersonates a business executive, employee, third party business, or other person with authority to request payments on behalf of a business.

10. In many instances, BEC scams begin when a legitimate user downloads malicious

[1] On December 5, 2019, one Bitcoin was equal to approximately $7,328.50 USD.

software (malware) by clicking on a malicious attachment or link in a spam or phishing e-mail; or acts upon a spoofed e-mail payment request crafted to look like it came from a company executive, employee, third party business, or another individual. An example of such a spoofed e-mail address from ceo@abc_company.com might appear as ceo@abc-company.com. In cases where malware or malicious links are used, the malware can provide criminals with full control of the user's computer, including access to passwords, documents, and e-mail. Alternatively, criminals can obtain a user's e-mail login information if it was stolen previously and sold online. In either case, the criminal's goal is to assume the identity of the legitimate user and request new payments or change the banking information of pending payments. Prior to executing the BEC scam, more sophisticated cyber criminals may even be able to monitor business communications for extended periods of time in order to understand operating procedures and the communication style of the individuals they want to impersonate. The payment transfers are sent to individuals commonly known as "money mules" to receive the funds in their bank accounts. These bank accounts usually belong to the money mules or businesses that were created by the individuals involved in the scam. The money mules are then able to distribute the money to other individuals involved in the scam either through additional transfers or from cash withdrawals.

11. In recent trends, criminals have been particularly active in targeting small to large companies and individuals which may transfer high-dollar funds in the course of business. As such, third party payroll companies, real estate transactions, legal services, and import/export companies are popular with criminals utilizing BEC scams.

12. Throughout this application, the below-listed set of terms, created by and commonly used by law enforcement, may be used to describe some of the techniques and tactics used to obtain the probable cause set forth in this Affidavit:

a. Business E-Mail Compromise (or BEC, as set forth above) - The term BEC refers to the impersonation of business executives by fraudsters who send phishing emails from seemingly legitimate sources, and requesting wire transfers to alternate, fraudulent accounts.

b. Phishing – The term "phishing" refers to an attempt to acquire sensitive information by masquerading as a trustworthy entity in electronic communications.

c. Spoofing – The term "spoofing" refers to the creation of email messages with a forged sender address.

V. FACTS ESTABLISHING PROBABLE CAUSE

13. Since in or about September 2019, the FBI has been conducting an investigation into a scheme that defrauded the Tukwila School District, which is based in the Western District of Washington, of over $6.5 million.

14. According to information obtained from the Tukwila School District, the District does business with Andy Johnson and Company, a commercial general contractor. Andy Johnson and Company is currently involved in modernizing middle and high schools in the Tukwila School District. Andy Johnson and Company's email address ends in "@ajcocontractors.com."

15. On or about August 21, 2019, the school district received a series of emails that purported to be from an accountant at Andy Johnson and Company. The emails were sent from an address ending in "@ajcocontractor.com," which differs from the actual e-mail address for Andy Johnson and Company only by a single letter (the "s" at the end of "contractor").

16. In the emails, the sender informed the Tukwila School District that he "would like to update the method of receiving payments for all of our invoices," requesting that payments made to Andy Johnson and Company be sent to an account held at Fifth Third Bank (ending in -7415). The Tukwila School District did not identify the discrepancy in the addresses and, on or about September 12, 2019, wired approximately $6,558,955.31 to the account at Fifth Third Bank. On or about September 23, 2019, the School District learned that they were victims of a fraud and reported the incident to law enforcement and to the School District's bank.

17. According to records obtained from Fifth Third Bank, the account ending in -7415 was opened on February 21, 2019, as a Business Standard Checking account, in the name of "William Sassman Logistics Construction." The address listed for SASSMAN on the signature card was 1255 University Avenue in Sacramento, California (defined above as the **SUBJECT RESIDENCE**). Additionally, the customer information associated with the account listed Sassman's address as 5150 Fair Oaks Blvd., Suite 101256, in Carmichael, California (defined above as the **SECONDARY SUBJECT LOCATION**).

18. After the $6,558,955.31 was transferred from the Tukwila School District to SASSMAN's Fifth Third Bank account, it was distributed to the following additional accounts:

Date	Amount	Account
9/16/19	$5,000	Transfer to Sassman's Fifth Third Bank Account (-5794)
9/17/19	$50.47	Payment to AT&T
9/17/19	$2,899.95	Payment to Macys Online
9/17/19	$5,663.46	Payment to Sassman's Discover Card
9/17/19	$9,510.55	Payment to Sassman's Capital One Card
9/18/19	$1,478.10	Payment to AT&T
9/18/19	$31,000	Check Issued to Philanthropic Concept's Account at JP Morgan Chase
9/19/19	$25,000	Payment to Sassman's Bitcoin of America Account
9/19/19	$496,204	Payment to Sassman's Bitcoin of America Account
9/20/19	$42.88	Payment to Shell in Carmichael, California
9/20/19	$3,024.99	Payment to the Apple Store in Sacramento, California
9/20/19	$195,000	Payment to Luxury Time NYC's JP Morgan Chase Account
9/20/19	$318,324	Payment to AVI & Co.'s TD Bank Account
9/23/19	$498,208	Payment to KC Inc.'s Frost Bank Account
9/23/19	$210,000	Check Issued to Philanthropic Concept's Account at JP Morgan Chase

19. As described in the table above, law enforcement has identified more than $750,000 that was transferred, or attempted to be transferred, to accounts associated with William SASSMAN. These accounts include the following:

a. SASSMAN's Fifth Third Bank Account (-5794): This account was opened on March 5, 2019 as a Business Money Market Account, associated with the company Logistics Construction. The address listed for SASSMAN on the signature card for the account was 1255 University Avenue in Sacramento, California (the **SUBJECT RESIDENCE**). On September 25, 2019, funds were

transferred back from SASSMAN's -5794 account to SASSMAN's -7415 account at Fifth Third Bank.

b. SASSMAN's Discover Card: This account was opened on August 10, 2018. On the statements for this account, SASSMAN's mailing address was listed as 5150 Fair Oaks Blvd., Suite 101, #256, in Carmichael, California (the **SECONDARY SUBJECT LOCATION**).

c. SASSMAN's Capital One Card: This account was opened on August 25, 2017. On the statements for this account, SASSMAN's mailing address was listed as 5150 Fair Oaks Blvd., Suite 101-294, in Carmichael, California.

d. SASSMAN's Bitcoin of America Account: Bitcoin of America is a cryptocurrency exchange, allowing users to purchase bitcoin and other digital currencies. This account was opened on September 17, 2019. The address listed for SASSMAN was 5150 Fair Oaks Blvd., Unit 101-256, in Carmichael, California (the **SECONDARY SUBJECT LOCATION**).

e. Philanthropic Concepts' JP Morgan Chase Account: Philanthropic Concepts, Inc. was incorporated in the State of California on September 14, 2016. On the incorporation records, the Agent for Service of Process was listed as William SASSMAN at 5150 Fair Oaks Blvd., Suite 101-256, in Carmichael, California (the **SECONDARY SUBJECT LOCATION**). As described herein, SASSMAN informed a Fifth Third Bank representative that this was his account.

20. As described in the above table, additional funds were sent to individuals and entities that do not appear to be associated with SASSMAN. For example, on September 23, 2019, $498,208 was transferred to KC Inc.'s Frost Bank Account. This account was opened on August 3, 2019 in the name of E.K. After receiving these funds, E.K. attempted to transfer $249,000 to an account at Coinbase, a cryptocurrency exchange. After the Tukwila School District reported the fraudulent transfer, Frost Bank personnel contacted E.K., who offered no reasonable explanation for the source of the funds. E.K. signed an authorization, allowing Frost Bank to return the funds to Fifth Third Bank.

///

21. As described in the table above, law enforcement also identified two transactions totaling roughly $500,000 that went to two stores specializing in luxury jewelry and watches located in New York City, NY. One transaction of $195,000 was sent to "Luxury Time NYC" on September 20, 2019. Another transaction of $318,324 was sent to "AVI & Co." also on September 20, 2019.

22. After the Tukwila School District reported the fraudulent transfer, Fifth Third Bank froze SASSMAN's accounts. On or about September 24, 2019, a person identifying himself as SASSMAN contacted Fifth Third Bank personnel to inquire why his accounts had been blocked. Fifth Third Bank personnel asked SASSMAN about the $6,448,995.33 deposit from the Tukwila School District. SASSMAN responded that these funds represented payment for a contract his company had been awarded involving a school in Missouri. SASSMAN explained that the outgoing payments were made to pay vendors for materials and supplies.

23. When confronted with the Tukwila School District's report that these funds were fraudulently transferred, SASSMAN advised Fifth Third Bank personnel that he had been caught up in a fraudulent employment scam involving an individual named Michael Heili. According to SASSMAN, he met Heili over the phone and communicated with him via Skype. Heili instructed SASSMAN to open the account at Fifth Third Bank. SASSMAN reportedly understood that his "role was to pay various vendors in order to procure construction supplies to build commercial construction buildings." SASSMAN explained that he would receive a 4% commission for his work and that Heili instructed him on where to send the funds. SASSMAN asked if the $210,000 check he deposited for Philanthropic Concepts, Inc., which SASSMAN identified as his account, would be refused. SASSMAN further indicated that he was willing to assist with the investigation. SASSMAN explained that he recorded everything on Skype and provided Fifth Third Bank personnel with a copy of Michael Heili's driver's license and passport.

24. As of October 30, 2019, Fifth Third Bank was able to recover $5,519,414.49 of the funds fraudulently transferred to SASSMAN's account and has returned them to the Tukwila School District. Additionally, pursuant to a seizure warrant issued on September 27,

2019 in the Western District of Washington, law enforcement seized an additional $496,204 from SASSMAN's Bitcoin of America account. Law enforcement is continuing to investigate where the remaining $643,336.82 is located.

A. SASSMAN's Involvement in the Fraud

25. Law enforcement identified William SASSMAN after accounts, held in his name, received a portion of the funds stolen from the Tukwila School District. Law enforcement has reviewed the activity in a portion of these accounts, which list charges incurred in the Sacramento, California region, where SASSMAN is believed to reside.

a. For example, the charges incurred on SASSMAN's Discover card predominately related to businesses in the Sacramento, California region, including restaurants, gas stations, and retail locations.

b. Similarly, the debit card linked to SASSMAN's Fifth Third Bank account (-7415) was predominately used at businesses in the Sacramento, California region, including grocery stores, laundries, and coffee shops.

c. Additionally, a portion of the funds transferred from the Tukwila School District to SASSMAN's Fifth Third Bank account (-7415) were used at the Apple Store and Shell gas station in Sacramento, California.

26. Law enforcement is continuing to investigate whether other individuals were involved in sending fraudulent emails to the Tukwila School District or distributing the funds received. For the reasons explained below, it is possible that one or more persons, in addition to SASSMAN may have played a role in defrauding the Tukwila School District.

a. The email addresses used to communicate with the Tukwila School District were registered to domain name registrars, which provide anonymizing services, allowing their users to avoid including identifying information in Whois databases and providing forwarding and filtering email services shielding users' true email address from distribution. According to information obtained from these registrars, the subscriber associated with one of the email addresses used to communicate with the Tukwila School District is "billyg025842745" using an Internet Protocol ("IP") address registered to a Virtual Private Network ("VPN"). The subscriber associated with another email address used to communicate with

the Tukwila School District was identified as C.L. using an IP address registered to a provider in the British Virgin Islands.

b. Additionally, records obtained from Bitcoin of America indicate that SASSMAN logged into his account more than 15 times between September 17, 2019 and September 24, 2019. While the IP addresses used on the two initial logins for this account belong to a subscriber, L.C., in the Sacramento, California region, other IP addresses resolve back to a subscriber in the Dinuba, California area. The remainder of the IP addresses used to log into the account are registered to VPN providers or to a telecommunications company operating in the United Kingdom. The subscriber associated with at least one of those VPN providers was listed as K.A., using IP addresses registered to providers in Hong Kong and China.

c. As part of their anti-money laundering protocols, SASSMAN was required to submit three photographs when opening his Bitcoin of America account, each selfies of SASSMAN holding certain documentation: (1) Payment Amount: $496,204; (2) Payment Date: Sep. 19, 2019; and (3) Originating Party Details (Debit Account): William SASSMAN [account number ending in "7415"]. I have reviewed a copy of SASSMAN's California State driver's license and have determined that the person in these photographs resembles William SASSMAN. However, it also appears that these pictures are digitally altered—instead of taking three separate pictures, the user simply cut and pasted the relevant document into an existing selfie of SASSMAN. Additionally, the bank records submitted when opening the account also appear to have been altered, since SASSMAN did not hold accounts at the banks provided or the account numbers referenced belonged to other customers.

d. Finally, on SASSMAN's credit reports, and a portion of his financial accounts, SASSMAN has reported that he has been the victim of identity theft. SASSMAN's Discover card also lists various disputed charges.

B. The SUBJECT RESIDENCE

27. Although SASSMAN frequently lists his mailing address as 5150 Fair Oaks Blvd., Unit 101-256, in Carmichael, California (the **SECONDARY SUBJECT LOCATION**) for the following reasons law enforcement believes that SASSMAN actually resides at 1255

University Avenue, Unit 221, in Sacramento, California (the **SUBJECT RESIDENCE**). Notably, the Carmichael address is a P.O. Box held at a The UPS Store.

28. SASSMAN's address is listed as 1255 University Avenue, Unit 221, in Sacramento, California (the **SUBJECT RESIDENCE**) on the following documents:

a. On the signature card for SASSMAN's Fifth Third Bank accounts (without the unit number specified);

b. On the utility record submitted when SASSMAN opened a Bitcoin of America account;

c. On a loan application submitted in SASSMAN's name to State Farm;

d. On SASSMAN's Comcast account, which, as described below, was used to log into an email account associated with SASSMAN;

29. On December 26, 2019, an FBI surveillance team observed SASSMAN go from the **SUBJECT RESIDENCE**. Specifically, at 10:03am, SASSMAN departed the **SUBJECT RESIDENCE** in a Toyota Tundra and drove to First US Community Credit Union at 580 University Ave. Sacramento, CA, 95825. Then, at 12:09pm, SASSMAN departed the **SUBJECT RESIDENCE** with an unknown female in the same Toyota Tundra and drove to a UPS Store located at 5150 Fair Oaks Ave. #101 (the **SECONDARY SUBJECT LOCATION**). The Toyota Tundra was last observed traveling north on Fair Oaks Ave. near Marconi Ave. after departing the UPS Store.

30. Law enforcement has identified at least two email addresses for SASSMAN, listed in the contact information on SASSMAN's financial accounts: drsassman@protonmail.com and drsassman@gmail.com. The latter email address is listed in the contact information for SASSMAN's Discover card.

31. According to information obtained from Google, the email address drsassman@gmail.com was created on April 11, 2016, and the subscriber listed on the account is "Dr. Will." The recovery email listed for the account is drsassman@protonmail.com. Since the account was opened, it has been logged into on

multiple occasions. At least three of those logins, occurring in July and September 2019, used IP addresses registered to SASSMAN's Comcast account. The address listed on that account was 1255 University Ave., Apt. 221, in Sacramento, California (the **SUBJECT RESIDENCE**). Additionally, there were numerous logins from IP addresses that were registered to VPN providers and a telecommunications provider located in the United Kingdom.

C. The SECONDARY SUBJECT LOCATION

32. SASSMAN lists his mailing address as 5150 Fair Oaks Blvd., Unit 101-256 in Carmichael, California (the **SECONDARY SUBJECT LOCATION**) on the following documents:

a. On customer information associated with SASSMAN's Fifth Third Bank accounts;

b. On the signature card for SASSMAN's River City Bank account;

c. On a loan application submitted in SASSMAN's name to State Farm;

d. On SASSMAN's Discover Card Statements;

e. On SASSMAN's Bitcoin of America Account customer information;

f. On SASSMAN's USAA Federal Savings Bank accounts statements

g. On the signature card for Philanthropic Concepts' JP Morgan Chase Account;

33. As discussed above, on December 26, 2019 at 12:09pm an FBI surveillance team observed SASSMAN depart the **SUBJECT RESIDENCE** with an unknown female and drive to the **SECONDARY SUBJECT LOCATION.**

D. Additional Fraudulent Schemes Linked to SASSMAN

34. In addition to defrauding the Tukwila School District, SASSMAN is also linked to additional alleged fraudulent activity.

35. For example, on August 9, 2019, a vehicle loan application was submitted for SASSMAN for a 2019 Ford F150 in the amount of $41,725. As part of that application a 2018 W-2 was submitted for SASSMAN. State Farm personnel determined that the W-2 contained fraudulent data, since the social security wages were listed as $326,581,

///

exceeding the maximum taxable earnings amount of $128,400 for 2018. State Farm declined to issue the vehicle loan.

36. Similarly, as part of the account opening records for SASSMAN's Bitcoin of America account, a 2018 W-2 was submitted for SASSMAN. Again, this W-2 listed SASSMAN's adjusted gross income as $1,900,000 and withholdings of $639,031. Based on a review of SASSMAN's residence (which appears to be a rented apartment), and the low level of spending reflected in his accounts, law enforcement believe that the W-2 form was likely falsified.

37. Finally, in 2011, SASSMAN was convicted of executing a Ponzi scheme and ordered to pay $4.45 million in restitution to 48 victims. As part of that case, investigators determined that SASSMAN sent over $200,000 to individuals based in Nigeria.

E. Request for Warrant

38. For at least the following reasons, there is probable cause to believe that the **SUBJECT RESIDENCE** contains evidence, instrumentalities, or proceeds of the crimes under investigation.

a. First, the crimes under investigation necessarily involve the use of computers or other electronic devices. For example, the perpetrators sent fraudulent emails to the Tukwila School District, the individual who identified himself as SASSMAN to Fifth Third Bank explained that he'd been communicating with a partner via Skype and telephone, and an account was opened online in SASSMAN's name at Bitcoin of America. Additionally, as described herein, in order to open accounts in SASSMAN's name, documents that appear to have been digitally altered were submitted and multiple VPN services and anonymizing domain name registrars were used. SASSMAN has a Comcast internet account registered to the **SUBJECT RESIDENCE** and, based on my training and experience, I know that individuals typically store their personal cell phones and computer devices in their homes.

b. Furthermore, proceeds of the crimes may be located in the **SUBJECT RESIDENCE**. For example, after receiving funds from the Tukwila School

District, SASSMAN's Fifth Third Bank debit card was used to make a $3,024.99 purchase at the Apple Store in Sacramento, California. According to Apple, these funds were used to purchase a MacBook Pro and two accessories. According to records obtained from Google, an iPhone and three Macintosh computers have been used to access the email account drsassman@gmail.com.

39. In addition, the investigative team plans to interview SASSMAN outside of his residence before or during the search of such residence. As such, I am requesting a warrant to search SASSMAN for evidence of the above-referenced crimes that may be contained on his person, such as his personal cellular phone. I know from my training and experience that individuals usually carry their personal cellular phones on them. As such, I am requesting the ability to search him for his personal cellular phone and other evidence he may have on his person when I or other case agents attempt to interview him.

40. In addition, there is probable cause to believe that the **SECONDAY SUBJECT LOCATION** contains evidence, instrumentalities, or proceeds of the crimes under investigation for the following reason. Financial account records, business records, and purchased products, among other records and items, are often sent through the mail. Digital storage devices can also be sent through the mail. The items remain in The UPS Store mailbox until the customer associated with the mailbox arrives to collect the items.

VI. SEARCH OF DIGITAL INFORMATION

41. As described above and in Attachment B, your affiant submits that computers, smart phones, and possibly other storage media will be found within the **SUBJECT RESIDENCE**, the **SECONDARY SUBJECT LOCATION**, and on the person of SASSMAN and there is probable cause to search and seize those items for the reasons stated below. Some of these electronic records might take the form of files, documents, and other data that is user-generated. Some of these electronic records, as explained below, might take a form that becomes meaningful only upon forensic analysis. Furthermore, your affiant submits that sufficient probable cause has been established to search and seize any online digital currency exchange platform accounts, and the data contained therein. Your affiant is also aware that individuals must use an electronic device to access e-mail and other communication facilities, and also to locate and

communicate with bitcoin exchangers. Users also must establish electronic wallets to receive and send bitcoins. These wallets are electronic in nature and may be stored on mobile devices (phones or tablets), external or removable media, and/or computers.

42. Based on my knowledge, training, and experience, your affiant is aware that a powered-on computer maintains volatile data. Volatile data can be defined as active information temporarily reflecting a computer's current state including registers, caches, physical and virtual memory, network connections, network shares, running processes, disks (floppy, tape and/or CD-ROM), and printing activity. Collected volatile data may contain such information as opened files, connections to other computers, passwords used for encryption, the presence of anti-forensic tools, or the presence of programs loaded in memory that would otherwise go unnoticed. Volatile data and its corresponding evidentiary value is lost when a computer is powered-off and unplugged.

43. Based on my knowledge, training, and experience, your affiant knows that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little to no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

44. Also, again based on your affiant's training and experience, wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations,

artifacts from operating system or application operation; file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information. Data on the storage medium not currently associated with any file can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

45. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for evidence that establishes how computers were used, the purpose of their use, who used them, and when.

46. Thus, the forensic analyst needs all assisting software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instructional manuals or other documentation and security devices. Moreover, searching computerized information for evidence or instrumentalities of crime commonly requires the seizure of the entire computer's input/output periphery devices (including related documentation, passwords and security devices) so that a qualified expert can accurately retrieve the system's data in a controlled environment.

47. In cases of this sort, laptop computers and/or smartphones are also used as instrumentalities of the crime to commit offenses involving fraud and the laundering of illegally obtained funds. Devices such as modems and routers can contain information

about dates, frequency, and computer(s) used to access the Internet. The laptop or smart phone may also have fingerprints on them indicating the user of the computer and its components.

48. Similarly, files related to fraud and the laundering of illegally obtained funds, as well as, the movement of currency found on computers and other digital communications devices are usually obtained from the Internet or the cellular data networks using application software which often leaves files, logs or file remnants which would tend to show the identity of the person engaging in the conduct as well as the method of location or creation of the data, search terms used, exchange, transfer, distribution, possession or origin of the files. Files that have been viewed via the Internet are sometimes automatically downloaded into a temporary internet directory or "cache". The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed internet pages or if a user takes steps to delete them. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

49. "User attribution" evidence can also be found on a computer and is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, and correspondence (and the data associated with the foregoing, such as file creation and last accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time. Your affiant knows from training and experience that digital software or hardware exists that allows persons to share digital access over wired or wireless networks allowing multiple persons to appear on the Internet from the same IP address. Examination of these items can reveal information about the authorized or unauthorized use of internet connection at the residence.

50. Searching the computer(s) for the evidence described in the attachment may require a range of data analysis techniques. For example, information regarding user attribution or internet use is located in various operating system log files that are not easily located or reviewed. In addition, a person engaged in criminal activity will attempt to conceal evidence of the activity by "hiding" files or giving them deceptive names. As explained above, because the warrant calls for records of how a computer has been used, what it has been used for, and who has used it, it is exceedingly likely that it will be necessary to thoroughly search storage media to obtain evidence, including evidence that is not neatly organized into files or documents. Just as a search of a premises for physical objects requires searching the entire premises for those objects that are described by a warrant, a search of this location (the computer) for the things described in this warrant will likely require a search among the data stored in storage media for the things (including electronic data) called for by this warrant. Additionally, it is possible that files have been deleted or edited, but that remnants of older versions are in unallocated space or slack space. This, too, makes it exceedingly likely that in this case it will be necessary to use more thorough techniques.

51. Based upon knowledge, training and experience, your affiant knows that a thorough search for information stored in storage media often requires agents to seize most or all storage media to be searched later in a controlled environment. This is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. Additionally, to properly examine the storage media in a controlled environment, it is often necessary that some computer equipment, peripherals, instructions, and software be seized and examined in the controlled environment. This is true because of the following:

a. The nature of evidence: As noted above, not all evidence takes the form of documents and files that can be easily viewed on-site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. Also, because computer evidence is extremely vulnerable to tampering and destruction (both from external sources and from code embedded

in the system as a "booby-trap"), the controlled environment of a laboratory is essential to its complete and accurate analysis.

b. The volume of evidence and time required for an examination: Storage media can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to peruse all the stored data to determine which particular files are evidence or instrumentalities of crime. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Reviewing information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

c. Technical requirements: Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on-site. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

d. Variety of forms of electronic media: Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

52. Based on the foregoing, and consistent with Rule 41(e)(2)(B), when persons executing the warrant conclude that it would be impractical to review the media on-site, the warrant I am applying for would permit seizing or imaging storage media that reasonably appear to contain some or all of the evidence described in the warrant, thus permitting its later examination consistent with the warrant. The examination may require techniques,

including but not limited to, computer-assisted scans of the entire medium that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant. The government seeks only to search digital devices owned and/or controlled by SASSMAN, and will not search and/or seize devices believed to belong to other individuals.

VII. REQUEST FOR SEALING

53. Finally, your affiant respectfully requests that this Court issue an order restricting, until further order of the Court, this case, to include, the Application and Search Warrant. I believe that restricting these documents are necessary to protect the integrity of the ongoing investigation, which is not yet overt. The items and information to be seized are relevant to an ongoing investigation into a criminal organization, and not all of the targets of this investigation will be searched at this time. Based upon my training and experience, your affiant has learned that online criminals actively search for criminal Affidavits and Search Warrants via the Internet and disseminate them to others actively seeking out information over the Web and other sources concerning law enforcement activity in this arena. Accordingly, premature disclosure of the contents of this Affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

[CONTINUED ON NEXT PAGE]

VIII. CONCLUSION

54. Based on the facts set forth in this Affidavit, I believe there is probable cause that evidence, fruits, proceeds, or instrumentalities of violations of Money Laundering and Conspiracy, in violation of Title 18, United States Code, Sections 1956 and 1957; Wire Fraud, in violation of Title 18, United States Code, Section 1343; Bank Fraud, in violation of Title 18, United States Code, Section 1344; Conspiracy to Commit Wire and Bank Fraud, in violation of Title 18, United States Code, Section 1349; and Fraud and Related Activity in Connection with Computers, in violation of Title 18, United States Code, Section 1030 are concealed in the locations identified in Attachments A-1, A-2, and A-3. Accordingly, I respectfully request the issuance of a search warrant authorizing the search of the locations described in Attachments A-1, A-2, and A-3, as well as the seizure of items described in Attachment B.

I swear, under the penalty of perjury, that the foregoing information is true and correct to the best of my knowledge, information, and belief.

Allison Boos
Special Agent
Federal Bureau of Investigations

Approved as to form:

/s/GRANT B. RABENN
GRANT RABENN
Assistant United States Attorney

Sworn and Subscribed to me on January 27, 2020

HONORABLE KENDALL J. NEWMAN
United States Magistrate Judge
Eastern District of California

ATTACHMENT A-2

LOCATION TO BE SEARCHED

PROPERTY TO BE SEARCHED – The person of WILLIAM SASSMAN, provided that he is located within the Eastern District of California at the time of the search. The search of SASSMAN is to include all bags, backpacks, notes, receipts, computers, digital devices, and digital media located on hi person or under his control, where the items specified in Attachment B may be found.

ATTACHMENT B

ITEMS TO BE SEIZED

The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed); photocopies or other photographic form; and electrical, electronic, and magnetic form (such as computers, hard drives, flash drives, tapes, cassettes, hard disks, floppy disks, diskettes, compact discs, CD-ROMs, DVDs, optical discs, Zip cartridges, printer buffers, smart cards, or electronic notebooks, or any other electronic storage medium) that constitute or contain evidence, instrumentalities, or fruits of violations of Money Laundering and Conspiracy, in violation of Title 18, United States Code, Sections 1956 and 1957; Wire Fraud, in violation of Title 18, United States Code, Section 1343; Bank Fraud, in violation of Title 18, United States Code, Section 1344; Conspiracy to Commit Wire and Bank Fraud, in violation of Title 18, United States Code, Section 1349; and Fraud and Related Activity in Connection with Computers, in violation of Title 18, United States Code, Section 1030 from August 2019 to the present.

1. All records relating to the violations described above, including:
   a. any and all documents, records or information relating to a Business E-Mail Compromise scheme;
   b. any and all documents, records or information relating to the laundering of illegally obtained funds;
   d. any and all documents, records or information relating to the transfer, purchase, sale or disposition of virtual currency;
   e. any and all documents, records, or information relating to the access, creation and maintenance of websites, e-mail accounts, or other means of remote electronic storage;
   f. any and all documents, records, or information relating to email accounts used in furtherance of these offenses;

g. any and all records or other items which are evidence of ownership or use of computer equipment, including, but not limited to, sales receipts, bills for internet access, handwritten notes and handwritten notes in computer manuals.

h. any and all records relating to indicia of occupancy, residency, and ownership or use of the properties to be searched, including, but not limited to, utility and telephone bills, cancelled envelopes, rental, purchase or lease agreements, identification documents, and keys;

i. any and all records of any address and/or telephone books, rolodex indicia, electronic organizers, telephone paging devices and the memory thereof, and any papers, records or electronic data reflecting names, addresses, telephone numbers, pager numbers of co-conspirators, sources of controlled substances and/or virtual currency, identifying information for customers purchasing controlled substances and/or virtual currency;

j. all bank records, checks, credit card bills, account information, safe deposit box information and other financial records;

k. all copies of income tax returns filed with the Internal Revenue Service (IRS) or the California Franchise Tax Board;

l. all records related to the purchase of real estate or other assets, or the leasing of storage units,

m. financial records including foreign and domestic banking records, ledger books, wire transfer instructions, and receipts for wire transfers,

n. all records related to the purchase of jewelry or gold,

o. bulk cash in excess of $1,000.

2. Any digital devices or other electronic storage media and/or their components used as a means to commit the violations described above, belonging to William SASSMAN, including:

a. any digital device or other electronic storage media capable of being used to commit, further, or store evidence or fruits of the offenses listed above;

b. any digital devices or other electronic storage media used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, cameras, printers, plotters, encryption devices, and optical scanners;

c. any magnetic, electronic or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, and personal digital assistants;

d. any documentation, operating logs and reference manuals regarding the operation of the digital device or other electronic storage media or software;

e. any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

f. any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and

g. any passwords, password files, seed words, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data.

3. For any digital device or other electronic storage media upon which electronically stored information that is called for by this warrant may be contained, or that may contain things otherwise called for by this warrant:

a. evidence of who used, owned, or controlled the digital device or other electronic storage media at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the digital device or other electronic storage media, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the digital device of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the digital device or other electronic storage media;

f. evidence of the times the digital device or other electronic storage media was used;

g. passwords, encryption keys, seed words, and other access devices that may be necessary to access the digital device or other electronic storage media;

h. documentation and manuals that may be necessary to access the digital device or other electronic storage media or to conduct a forensic examination of the digital device or other electronic storage media;

i. contextual information necessary to understand the evidence described in this attachment.

4. Records and things evidencing the use of an Internet Protocol (IP) address to communicate with the internet, including:

a. routers, modems, and network equipment used to connect computers to the internet;

b. records of Internet Protocol addresses used;

c. records of internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses.

5. Any and all hidden services accounts or encrypted chat applications used in furtherance of the offenses described above, including, but not limited to, darknet market accounts, associated darknet forum accounts, Tor-based email accounts, and Wickr handles and logins.

6. Any and all peer to peer (P2P) virtual currency trading platform accounts, with no legitimate or identified service provider to which legal process may be served, used in furtherance of the offenses described above, including, but not limited to, localbitcoins.com accounts or bitcoin-otc internet relay chat channel accounts.

7. Virtual currency in any format, including but not limited to, wallets (digital and paper), seed words, usernames and passwords, public keys (addresses) and private keys.

8. Fiat currency (U.S. dollars or other government issued currency).

9. Luxury jewelry or gold valued over $10,000.

10. Keys to storage units, suites, lockers and safe deposit boxes.

11. Firearms or other prohibited weapons.

THE SEIZURE OF DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA AND/OR THEIR COMPONENTS AS SET FORTH HEREIN IS SPECIFICALLY AUTHORIZED BY THIS SEARCH WARRANT, NOT ONLY TO THE EXTENT THAT SUCH DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA CONSTITUTE INSTRUMENTALITIES OF THE CRIMINAL ACTIVITY DESCRIBED ABOVE, BUT ALSO FOR THE PURPOSE OF CONDUCTING OFF-SITE EXAMINATIONS OF THEIR CONTENTS FOR EVIDENCE, INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED CRIME.

SEALED

UNITED STATES DISTRICT COURT

for the

Eastern District of California

In the Matter of the Search of)
)
)
The person of WILLIAM SASSMAN)
)
)
)

Case No. 2:20-SW-0100-KJN

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of California *(identify the person or describe the property to be searched and give its location)*:

SEE ATTACHMENT A-2, attached hereto and incorporated by reference.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B, attached hereto and incorporated by reference.

YOU ARE COMMANDED to execute this warrant on or before Feb 10, 2020 *(not to exceed 14 days)*

☑ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to: any authorized U.S. Magistrate Judge in the Eastern District of California.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of

Date and time issued: JAN 27, 2020 3:35 p.m.

Judge's signature

City and state: Sacramento, California

Kendall J. Newman, U.S. Magistrate Judge

Printed name and title

Return		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name of any person(s) seized:		

Certification

I swear that this inventory is a true and detailed account of the person or property taken by me on the warrant.

_____

Subscribed, sworn to, and returned before me this date.

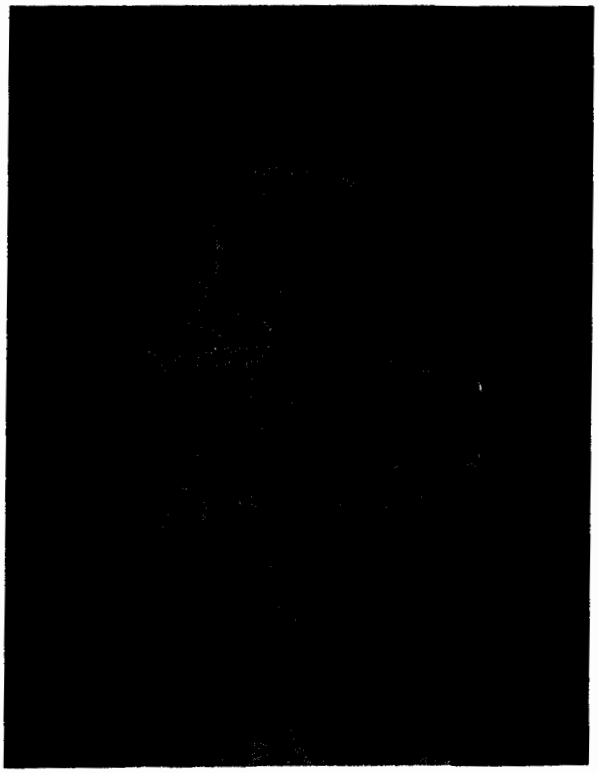
_____ Signature of Judge

_____ Date

ATTACHMENT A-2

LOCATION TO BE SEARCHED

PROPERTY TO BE SEARCHED – The person of WILLIAM SASSMAN, provided that he is located within the Eastern District of California at the time of the search. The search of SASSMAN is to include all bags, backpacks, notes, receipts, computers, digital devices, and digital media located on hi person or under his control, where the items specified in Attachment B may be found.



ATTACHMENT B

ITEMS TO BE SEIZED

The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed); photocopies or other photographic form; and electrical, electronic, and magnetic form (such as computers, hard drives, flash drives, tapes, cassettes, hard disks, floppy disks, diskettes, compact discs, CD-ROMs, DVDs, optical discs, Zip cartridges, printer buffers, smart cards, or electronic notebooks, or any other electronic storage medium) that constitute or contain evidence, instrumentalities, or fruits of violations of Money Laundering and Conspiracy, in violation of Title 18, United States Code, Sections 1956 and 1957; Wire Fraud, in violation of Title 18, United States Code, Section 1343; Bank Fraud, in violation of Title 18, United States Code, Section 1344; Conspiracy to Commit Wire and Bank Fraud, in violation of Title 18, United States Code, Section 1349; and Fraud and Related Activity in Connection with Computers, in violation of Title 18, United States Code, Section 1030 from August 2019 to the present.

1. All records relating to the violations described above, including:
   a. any and all documents, records or information relating to a Business E-Mail Compromise scheme;
   b. any and all documents, records or information relating to the laundering of illegally obtained funds;
   d. any and all documents, records or information relating to the transfer, purchase, sale or disposition of virtual currency;
   e. any and all documents, records, or information relating to the access, creation and maintenance of websites, e-mail accounts, or other means of remote electronic storage;
   f. any and all documents, records, or information relating to email accounts used in furtherance of these offenses;

g. any and all records or other items which are evidence of ownership or use of computer equipment, including, but not limited to, sales receipts, bills for internet access, handwritten notes and handwritten notes in computer manuals.

h. any and all records relating to indicia of occupancy, residency, and ownership or use of the properties to be searched, including, but not limited to, utility and telephone bills, cancelled envelopes, rental, purchase or lease agreements, identification documents, and keys;

i. any and all records of any address and/or telephone books, rolodex indicia, electronic organizers, telephone paging devices and the memory thereof, and any papers, records or electronic data reflecting names, addresses, telephone numbers, pager numbers of co-conspirators, sources of controlled substances and/or virtual currency, identifying information for customers purchasing controlled substances and/or virtual currency;

j. all bank records, checks, credit card bills, account information, safe deposit box information and other financial records;

k. all copies of income tax returns filed with the Internal Revenue Service (IRS) or the California Franchise Tax Board;

l. all records related to the purchase of real estate or other assets, or the leasing of storage units,

m. financial records including foreign and domestic banking records, ledger books, wire transfer instructions, and receipts for wire transfers,

n. all records related to the purchase of jewelry or gold,

o. bulk cash in excess of $1,000.

2. Any digital devices or other electronic storage media and/or their components used as a means to commit the violations described above, belonging to William SASSMAN, including:

a. any digital device or other electronic storage media capable of being used to commit, further, or store evidence or fruits of the offenses listed above;

b. any digital devices or other electronic storage media used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, cameras, printers, plotters, encryption devices, and optical scanners;

c. any magnetic, electronic or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, and personal digital assistants;

d. any documentation, operating logs and reference manuals regarding the operation of the digital device or other electronic storage media or software;

e. any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

f. any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and

g. any passwords, password files, seed words, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data.

3. For any digital device or other electronic storage media upon which electronically stored information that is called for by this warrant may be contained, or that may contain things otherwise called for by this warrant:

a. evidence of who used, owned, or controlled the digital device or other electronic storage media at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the digital device or other electronic storage media, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the digital device of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the digital device or other electronic storage media;

f. evidence of the times the digital device or other electronic storage media was used;

g. passwords, encryption keys, seed words, and other access devices that may be necessary to access the digital device or other electronic storage media;

h. documentation and manuals that may be necessary to access the digital device or other electronic storage media or to conduct a forensic examination of the digital device or other electronic storage media;

i. contextual information necessary to understand the evidence described in this attachment.

4. Records and things evidencing the use of an Internet Protocol (IP) address to communicate with the internet, including:

a. routers, modems, and network equipment used to connect computers to the internet;

b. records of Internet Protocol addresses used;

c. records of internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses.

5. Any and all hidden services accounts or encrypted chat applications used in furtherance of the offenses described above, including, but not limited to, darknet market accounts, associated darknet forum accounts, Tor-based email accounts, and Wickr handles and logins.

6. Any and all peer to peer (P2P) virtual currency trading platform accounts, with no legitimate or identified service provider to which legal process may be served, used in furtherance of the offenses described above, including, but not limited to, localbitcoins.com accounts or bitcoin-otc internet relay chat channel accounts.

7. Virtual currency in any format, including but not limited to, wallets (digital and paper), seed words, usernames and passwords, public keys (addresses) and private keys.

8. Fiat currency (U.S. dollars or other government issued currency).

9. Luxury jewelry or gold valued over $10,000.

10. Keys to storage units, suites, lockers and safe deposit boxes.

11. Firearms or other prohibited weapons.

THE SEIZURE OF DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA AND/OR THEIR COMPONENTS AS SET FORTH HEREIN IS SPECIFICALLY AUTHORIZED BY THIS SEARCH WARRANT, NOT ONLY TO THE EXTENT THAT SUCH DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA CONSTITUTE INSTRUMENTALITIES OF THE CRIMINAL ACTIVITY DESCRIBED ABOVE, BUT ALSO FOR THE PURPOSE OF CONDUCTING OFF-SITE EXAMINATIONS OF THEIR CONTENTS FOR EVIDENCE, INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED CRIME.